ЛІТЕРАТУРА

1. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016.
2. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.
3. oneM2M. Technical Specifications. 2021. URL: https://www.onem2m.org/technical/published-documents
4. IBM Research. Autonomous Machine-to-Machine Transactions. 2017.
5. European Union Agency for Cybersecurity (ENISA). Security and Resilience of Smart Contract Systems. 2020.
6. Markou C., Koutroumpis P. Legal and Regulatory Issues of Smart Contracts. Computer Law & Security Review. 2020.

УДК 347.6:341.231.14(477)

Петренко В.А.
студент першого курсу юридичного факультету
Західноукраїнський національний університет
Науковий керівник:
Поперечна Г.М.
Д.філ.(право), доцент, доцент кафедри
міжнародного та європейського права
Західноукраїнський національний університет

ЦИФРОВА БЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПРИВАТНОПРАВОВИХ ВІДНОСИНАХ. (ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУБ'ЄКТІВ ПРИВАТНОГО ПРАВА)

Стрімка цифровізація суспільних, економічних та правових процесів зумовила суттєве зростання обсягів обробки персональних даних у приватноправових відносинах. Активне впровадження електронних сервісів, дистанційних форм взаємодії, цифрових платформ та автоматизованих систем аналізу інформації істотно підвищило ризики порушення права особи на приватність. Особливої актуальності проблематика захисту персональних даних

набула в умовах пандемії COVID-19 та повномасштабної збройної агресії Російської Федерації проти України, які прискорили процеси цифровізації та перевели значну частину приватноправових відносин у кіберпростір [1, с. 12].

У сучасних умовах цифрова безпека та захист персональних даних виступають невід'ємною складовою забезпечення фундаментального права на повагу до приватного життя. У приватноправових відносинах, зокрема цивільних, трудових та господарських, персональні дані стають об'єктом постійної обробки, зберігання та передачі, що створює нові загрози несанкціонованого доступу, незаконного поширення та комерційного використання інформації про особу. Відсутність належних правових і технічних запобіжників у цифровому середовищі може призводити до істотного порушення прав та законних інтересів суб'єктів приватного права [2, с. 281].

Національне законодавство України у сфері захисту персональних даних ґрунтується на положеннях Конституції України, зокрема статті 32, яка гарантує право на невтручання в особисте і сімейне життя, а також на Законі України «Про захист персональних даних», що визначає принципи законності, цільового характеру, пропорційності та безпеки обробки інформації. Водночас чинні правові механізми залишаються фрагментарними та не завжди здатними ефективно реагувати на виклики, пов'язані з розвитком технологій *Big Data*, штучного інтелекту та транскордонного характеру обміну інформацією [3, с. 58].

Важливу роль у забезпеченні цифрової безпеки у приватноправових відносинах відіграють приватноправові інструменти, зокрема договірні положення про конфіденційність, умови обробки персональних даних, використання електронної ідентифікації та засобів автентифікації. Саме договірна автономія сторін дозволяє деталізувати обсяг прав і обов'язків щодо захисту інформації та запроваджувати превентивні механізми запобігання порушенням, що відповідає сучасним підходам до приватноправового регулювання цифрових відносин [4, с. 49-55].

Суттєвий вплив на розвиток національного законодавства у сфері захисту персональних даних мають міжнародні стандарти, зокрема Загальний регламент

Європейського Союзу про захист даних (*GDPR*) та Конвенція Ради Європи №108+. Зазначені акти встановлюють високі вимоги до безпеки обробки персональних даних, прозорості та відповідальності суб'єктів, що фактично формує орієнтир для гармонізації українського законодавства з європейськими стандартами [5].

Судова практика національних судів та Європейського суду з прав людини підтверджує, що держава має позитивний обов'язок забезпечувати ефективний захист персональних даних у приватному секторі, а порушення таких прав може бути підставою для цивільно-правової відповідальності та відшкодування моральної шкоди [6, с. 221]. Судова практика свідчить про послідовне посилення захисту персональних даних і приватного життя як на національному, так і на міжнародному рівнях. У рішенні Печерського районного суду м. Києва у справі № 757/29660/23-ц від 31.10.2023 визнано протиправним поширення ЗМІ фото та персональних даних адвоката без його згоди, встановлено наявність моральної шкоди та присуджено компенсацію, що підтверджує обов'язок приватних суб'єктів дотримуватися стандартів захисту персональних даних. Аналогічний підхід простежується у практиці ЄСПЛ: у справі Pietrzak and Bychawska-Siniarska and Others v. Poland (28.05.2024) Суд наголосив, що навіть саме існування законодавства про широке та неконтрольоване спостереження становить втручання у приватне життя, а у справі Guyvan v. Ukraine (06.11.2025) підкреслив позитивний обов'язок держави захищати осіб від неправомірного збору й обробки персональних даних, зокрема у трудових відносинах. Це свідчить про реальність загроз приватності у цифровому середовищі та необхідність комплексного підходу до забезпечення цифрової безпеки.

Отже, аналіз правових механізмів захисту персональних даних у приватноправових відносинах свідчить, що стрімкий розвиток цифрових технологій і активне використання персональної інформації суттєво підвищують ризики порушення приватності та кібербезпеки, що зумовлює необхідність ефективного правового регулювання на національному й міжнародному рівнях. Захист персональних даних у приватному секторі забезпечується нормами

національного законодавства України та міжнародними стандартами, зокрема *GDPR*, Конвенцією Ради Європи №108+ і Будапештською конвенцією, які визначають правила обробки даних і відповідальність за їх порушення. Персональні дані є складовою немайнових прав, а їх неправомірне використання може спричиняти цивільно-правову, адміністративну та кримінальну відповідальність, що підкреслює потребу подальшого вдосконалення механізмів правозастосування. Таким чином, забезпечення цифрової безпеки у приватноправових відносинах потребує комплексного підходу, який поєднує договірні інструменти, технічні засоби захисту та узгоджене застосування національних і міжнародних правових стандартів з метою збалансування прав суб'єктів даних, інтересів бізнесу та вимог національної безпеки.

ЛІТЕРАТУРА

1. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 8-14.
2. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2010. 281 p.
3. Тарасенко В.О. Правовий механізм захисту персональних даних в кіберпросторі. *Юридичний науковий електронний журнал.* 2025. № 3. С. 313-316.
4. Кузнєцова Н. С., Кохановська О. В. Сучасне приватне право України: вектори європейського розвитку. *Вісник Національної академії правових наук України.* 2016. № 3 (86). С. 49–55.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (date of reference 21.01.2026).
6. Посібник з європейського права у сфері захисту персональних даних. Агенція Європейського Союзу з питань основоположних прав, Рада Європи. К. :